On Gigantic Pairs of Minimal Clones (Models of Computation and Algorithms)

AUTHOR(S):

Machida, Hajime; Rosenberg, Ivo G.

数理解析研究所講究録
1093巻 1999年 87-92

On Gigantic Pairs of Minimal Clones

町田 元 (Machida, Hajime)* and Ivo G. Rosenberg†
* Hitotsubashi University, † Université de Montréal

1 Introduction and Preliminary Observations

In this paper we deal with some problem from the "clone theory", which stands as a research area in multiple-valued logic and universal algebra. Roughly speaking, a clone is a set of operations (functions) which is closed under composition.[†1] As an introduction to our problem, one may describe the motivation of the problem in very simple and elementary way as follows:

" Is it possible to generalize the set of operations $\{\mathrm{NOT}, \mathrm{OR}\}$ on the base set $\{0,1\}$ to a set of operations on the base set $\{0,1,\ldots,k-1\}$ $(k \geq 2)$? "

This is certainly simple, but is too simple and almost nothing is conveyed from this statement. In order to state the problem more clearly and definitely, we extract the following properties from the set $\{\mathrm{NOT}, \mathrm{OR}\}$.

(i) $\{\mathrm{NOT}\}$ generates a minimal clone †.

(ii) $\{\mathrm{OR}\}$ generates a minimal clone.

(iii) $\{\mathrm{NOT}, \mathrm{OR}\}$ is complete † (*i.e.*, generates all the operations).

Our problem asks if these properties can be generalized into k-valued case.

Problem : Does there exist a pair of operations f, g having the above three properties (i), (ii) and (iii), in place of NOT and OR, for arbitrary $k \geq 2$?

We shall call this problem **Szabó's problem** named after the first person who took up the problem.

Now, we shall fix $k \geq 2$ and set $\boldsymbol{k} = \{0,1,\ldots,k-1\}$. Let two operations $f(x_1,\ldots,x_m), g(x_1,\ldots,x_n)$ on $\boldsymbol{k}$ satisfy the three properties (i), (ii) and (iii), that is,

(i) $[f]$ is a minimal clone.

(ii) $[g]$ is a minimal clone.

(iii) $[f,g] = \mathcal{O}_k$ (= the set of all operations on $\boldsymbol{k}$)†.

Here, for a set S of operations, $[S]$ † denotes the set of all operations which are generated by S.

Moreover, we assume that both f and g depend on every variable, *i.e.* f is an essetially m-variable operation and g is an essentially n-variable operation.

A pair of operations (f,g) which satisfies the above conditions (i), (ii) and (iii) shall be called a **gigantic pair** † of minimal operations.

In the following, some introductory observations are given on the conditions for a pair (f,g) to be a gigantic pair.

Claim 1 : If $f(a,\ldots,a) = a$ and $g(a,\ldots,a) = a$ hold for some $a \in \mathbf{k}$, $[f,g]$ is not complete.

This is immediate from the fact that $f(a,\ldots,a) = a$ and $g(a,\ldots,a) = a$ imply $h(a,\ldots,a) = a$ for any operation h which is obtained by compositions of f and g.

[1] The symbol † means that a precise definition for the term is given in Section 2.

Claim 2 : If $m \geq 2$ and $[f]$ is a minimal clone, $f(x,\ldots,x) = x$ for every $x \in \boldsymbol{k}$. (Such operation f is called idempotent †.) The same is true for g, of course.

This is because if $f(a,\ldots,a) = b$ $(a \neq b)$ for some a, b, $[h] \subset [f]$ holds for unary operation h defined by $h(x) = f(x,\ldots,x)$ and $[f]$ cannot be a minimal clone.

According to Claims 1 and 2, at least one operation f or g must be unary operation. On the other hand, the condition (iii) clearly requires that at least one operation must not be unary. These considerations lead to the following.

Claim 3 : Let $m \leq n$. Then f is a unary operation $(m = 1)$ and g is an idempotent operation with 2 or more variables $(n \geq 2)$.

The following fact characterizing a unary operation which generates a minimal clone is well-known and easy to verify.

Claim 4 : Suppose a unary operation f is not the identity operation. $[f]$ is a minimal clone if and only if the following (i) or (ii) holds.

(1) f is not surjective and the restriction of f to Image(f) is the identity operation on Image(f).

(2) f is a permutation of prime order.

As we have seen that g is an idempotent operation, f must be an operation of type (2) in Claim 4 in order to make the condition (iii) hold. Moreover, one can assert, w.l.o.g., that

$$f = (0\ 1\ \ldots\ p-1)(p\ p+1\ \ldots\ 2p-1)\ldots((\ell-1)p\ \ldots\ \ell p-1)$$

where $k = \ell p$.

Due to the similar argument with Claim 1 we have:

Claim 5 : If $f(S) \subseteq S$ and $g(S,\ldots,S) \subseteq S$ for some proper subset $S \subset \boldsymbol{k}$, $[f,g]$ is not complete.

Thus, when f is the operation given above and $\ell > 1$, g must be an operation which satisfy, *e.g.*,

$$g(\{0,1,\ldots,p-1\},\ldots,\{0,1,\ldots,p-1\}) \not\subseteq \{0,1,\ldots,p-1\}.$$

So far, what we have discussed is merely the very basic properties that operations f and g must satisfy. These observations are the first step of our study. By extending the considerations more deeply, we have obtained the following results which will be stated in detail in Section 3.

(1) We obtained a necessary and sufficient condition for a pair of operations (f,g) to be a gigantic pair. (Theorem 3.1)

(2) We verified that a gigantic pair really exists for every $k \neq 2^t (t > 1)$ by constructing such pairs. (Theorem 3.3) In our construction g is the join operator corresponding to some semilattice †. (Fig. 1) The reader is invited to verify that the premiss in Claim 5 does not hold for this operation g and the above operation f.

In the following, due to the lack of space, we shall give only definitions and theorems, but (almost) no proofs.

2 Definitions

Let $\mathcal{O}_k^{(n)}$ be the set of all n-ary operations from $\boldsymbol{k}^n$ into $\boldsymbol{k}$ and let $\mathcal{O}_k (= \mathcal{O}_A) = \bigcup_{n=1}^{\infty} \mathcal{O}_k^{(n)}$. Let $\mathcal{J}_k$ be the set of all projections pr_i^n $(1 \leq i \leq n)$ over $\boldsymbol{k}$ where pr_i^n is defined as $pr_i^n(x_1,\ldots,x_i,\ldots,x_n) = x_i$

for arbitrary $(x_1, \ldots, x_n)$ in $\boldsymbol{k}^n$.

An operation $f \in \mathcal{O}^{(n)}$ is *idempotent* if $f(x, \ldots, x) \approx x$. (Here and in the sequel, $\approx$ denotes an identity over $\boldsymbol{k}$, *i.e.*, $f(x, \ldots, x) \approx x$ means $f(x, \ldots, x) = x$ for all $x \in \boldsymbol{k}$.)

Definition 2. 1 *A subset C of $\mathcal{O}_k$ is a* **clone** *on $\boldsymbol{k}$ if* (i) *C contains $\mathcal{J}_k$ and* (ii) *C is closed under (functional) composition.*

Definition 2. 2 *For a subset S of $\mathcal{O}_k$, the clone* **generated by** *S is defined to be the smallest clone containing S. It is denoted by $[S]$. A set S is* **complete** *if $[S] = \mathcal{O}_k$,* i.e., *every operation in $\mathcal{O}_k$ can be obtained by composing operations in $S \cup \mathcal{J}_k$.*

Definition 2. 3 *A clone C on $\boldsymbol{k}$ is a* **minimal clone** *if* (i) *$C \neq \mathcal{J}_k$ and* (ii) *$\mathcal{J}_k \subset C' \subseteq C$ implies $C' = C$ for any clone C' on $\boldsymbol{k}$.*

Definition 2. 4 *An operation f on $\boldsymbol{k}$ is* **minimal** *if* (i) *it generates a minimal clone and* (ii) *every operation from $[f]$ whose arity is smaller than the arity of f is a projection.*

Theorem 2. 1 *[Ro 86] Every minimal operation belongs to one of the following five types:*

1) Unary operations f (i.e., *selfmaps of $\boldsymbol{k}$) such that either (i) $f^2 (= f \circ f) = f$ or (ii) f is a permutation of prime order p* (i.e., *$f^p = id$*).

2) Idempotent binary operations; i.e., *$f \in \mathcal{O}^{(2)}$ such that $f(x, x) \approx x$.*

3) Majority operations; i.e., *$f \in \mathcal{O}^{(3)}$ such that $f(x, x, y) \approx f(x, y, x) \approx f(y, x, x) \approx x$.*

4) Semiprojections (or quasiprojections); i.e., *$f \in \mathcal{O}^{(n)}$ $(3 \leq n \leq k)$ such that there exists i $(1 \leq i \leq n)$ satisfying $f(a_1, \ldots, a_n) = a_i$ whenever $a_1, \ldots, a_n \in \boldsymbol{k}$ are not pairwise distinct.*

5) If $k = 2^m$, the ternary operations $f(x, y, z) \approx x + y + z$ where $< \boldsymbol{k}\,; + >$ is an elementary 2-group (i.e., *the additive group of an m-dimensional vector space over GF(2)).*

Definition 2. 5 *A pair (f, g) of minimal operations is called* **gigantic** *if $\{f, g\}$ is complete. (i.e., $[f, g] = \mathcal{O}$.)*

The following terminology is from universal algebra.

Definition 2. 6 $\mathbf{A} = < A; F >$ *is an* **algebra** *if A is a set and F is a set of finitary operations defined over and taking values in A. When $F = \{f_1, \ldots, f_t\}$, $\mathbf{A}$ is also expressed as $< A; f_1, \ldots, f_t >$. For an algebra $\mathbf{A} = < A; F >$, a subset B of A is a* **subuniverse** *of $\mathbf{A}$ if B is closed under every operation f in F. A subuniverse B of $< A; F >$ is a* **proper** *subuniverse if $\phi \subset B \subset A$.*

For an algebra $\mathbf{A} = < A; F >$, θ is a **congruence** *of $\mathbf{A}$ if θ is an equivalence relation on A and satisfies the property that for every operation f in F, if f is n-ary, $x_1 \theta y_1, \ldots, x_n \theta y_n$ implies $f(x_1, \ldots, x_n) \theta f(y_1, \ldots, y_n)$ for all $x_1, \ldots, x_n, y_1, \ldots, y_n \in A$. A congruence θ of $\mathbf{A}$ is* **proper** *if θ is not a trivial equivalence relation. An algebra $\mathbf{A}$ is* **simple** *if it has no proper congruences.*

Moreover, for an algebra $\mathbf{A} = < A; F >$, φ is an **automorphism** *of $\mathbf{A}$ if φ is a permutation on A and satisfies the property that for every operation f in F, if f is n-ary, $f(\varphi(x_1), \ldots, \varphi(x_n)) = \varphi(f(x_1, \ldots, x_n))$ for all $x_1, \ldots, x_n \in A$. The set of all automorphisms of $\mathbf{A}$ is denoted by* Aut $\mathbf{A}$. *An automorphism φ is* **proper** *if φ is not an identity permutation id_A of A.*

Finally in this subsection, we supply some definitions concerning relations.

Definition 2. 7 *For a set A, an h-***ary relation** *on A is a subset of the Cartesian product A^h. For an n-ary operation f in $\mathcal{O}_A$ and an h-ary relation ρ on A, f is said to* **preserve** *ρ if $(x_{1j}, x_{2j}, \ldots, x_{hj}) \in \rho$ for every $j = 1, 2, \ldots, n$ implies $(f(x_{11}, x_{12}, \ldots, x_{1n}), \ldots, f(x_{h1}, x_{h2}, \ldots, x_{hn})) \in \rho$.*

Definition 2. 8 *Let $k = h^m$ where $h > 2$ and $m \geq 1$. A set $T = \{\theta_1, \ldots, \theta_m\}$ of equivalence relations on $\boldsymbol{k}$ is an h-***regular system** *if* (i) *each block (equivalence class) of every θ_i has h elements and* (ii) *if B_i is a block of θ_i for all $i = 1, \ldots, m$ then $|B_1 \cap \cdots \cap B_m| \geq 1$. Next, the relation determined by T is the relation λ_T defined as the set of all $(a_1, \ldots, a_h) \in \boldsymbol{k}^h$ such that for each $i = 1, \ldots, m$ it holds that $a_r \theta_i a_s$ for some $1 \leq r < s \leq h$.*

3 Main Results

Definition 3.1 *For a divisor p of k denote by F_p the set of all permutations of $\mathbf{k}$ with $\ell := k/p$ cycles of length p. Let $f \in F_p$ have cycles $C_0, \dots, C_{\ell-1}$.*

An equivalence relation θ on $\mathbf{k}$ is **transversal** *to f if there exist* 1) *an equivalence relation λ on $\boldsymbol{\ell}$ distinct from the least equivalence relation on $\boldsymbol{\ell}$ and* 2) *an element $c_i \in C_i$ for each $i \in \boldsymbol{\ell}$ such that*

$$\theta = \{(f^m(c_i), f^m(c_j)) \mid i \lambda j,\ 0 \le m \le p-1\}.$$

A permutation ψ of $\mathbf{k}$ is **orthogonal** *to f if* 1) *$\psi \in F_q$ for some prime divisor q of k,* 2) *$f \circ \psi = \psi \circ f$ and* 3) *if $q \neq p$ then each cycle of ψ meets every C_i in at most a singleton.*

Now, we characterize gigantic pairs.

Theorem 3.1 *Let $f \in \mathcal{O}^{(m)}$ and $g \in \mathcal{O}^{(n)}$ where $m \le n$ and let $\mathbf{A} :=< \mathbf{k}; g >$. Then the pair (f, g) is gigantic if and only if*

(i) *$m = 1$ and $f \in F_p$ for some prime divisor p of k (with cycles $C_0, \dots, C_{\ell-1}$),*

(ii) *$n > 1$ and g is minimal,*

(iii) *$C_{i_1} \cup \dots \cup C_{i_h}$ is not a proper subuniverse of $\mathbf{A}$ for any $0 \le i_1 < \dots < i_h \le \ell - 1$,*

(iv) *No congruence of $\mathbf{A}$ is transversal to f,*

(v) *No automorphism of $\mathbf{A}$ is orthogonal to f,*

(vi) *Let $k = h^m$ where $h > 2$ and $m > 1$. If there exist:* a) *a permutation φ of $\boldsymbol{m}$ of order 1 or p and permutations $f_0, \dots, f_{m-1}$ of $\mathbf{h}$ such that*
   α) $f_{d_0} f_{d_1} \cdots f_{d_{p-1}} = id_{\mathbf{h}}$ for each cycle $(d_0 \dots d_{p-1})$ of φ,
   β) for every fixed point i of φ the permutation f_i is of order 1 or p and
   γ) for some fixed point j of φ the permutation f_j is fixed-point-free and of order p
   and b) *a bijection*

$$\psi : x \longmapsto \widehat{x} = (x^{(0)}, \dots, x^{(m-1)})$$

of $\mathbf{k}$ onto $\mathbf{h}^m$ such that for all $x \in \mathbf{k}$

$$\widehat{f(x)} = (f_0(x)^{(\varphi(0))}, \dots, f_{m-1}(x)^{(\varphi(m-1))}),$$

then g does not preserve the h-ary relation

$$\{(a_1, \dots, a_h) \in \mathbf{k}^h \mid \#\{a_1^{(i)}, \dots, a_p^{(i)}\} < p-1 \ \text{ for every } \ i = 0, \dots, m-1\}.$$

(vii) a) *Let $k = p^m$,* b) *let $x \longmapsto \widehat{x}$ be a bijection from $\mathbf{k}$ onto $\mathbf{p}^m$ (the latter considered as the set of all $m \times 1$ matrices over $\mathbf{p}$),* c) *let for all $x \in \mathbf{k}$*

$$\widehat{f(x)} = A\widehat{x} + B$$

where $A = P^{-1}JP$, $B = P^{-1}B'$ with P a nonsingular (over GF(p)) $m \times m$ matrix over $\mathbf{p}$, J the $m \times m$ Jordan matrix with diagonal $(1, \dots, 1)$ and blocks of sizes $\ell_1, \dots, \ell_h$ and $B' = (b_1, \dots, b_m) \in \mathbf{p}^m$ is such that

$$(I + J + J^2 + \dots + J^{p-1})B' = O_{m \times 1},$$

and $b_{\ell_1 + \dots + \ell_u} \neq 0$ for some $1 \le u \le h$. Then g does not preserve the quaternary relation

$$\{(x, y, z, t) \in \mathbf{k}^4 \mid \widehat{t} = \widehat{x} \ominus \widehat{y} \oplus \widehat{z}\}.$$

The proof of Theorem 3.1 heavily relies on the following theorem.

Theorem 3. 2 [Ro 70B] *For a set B of surjective operations containing an essentially more than unary operation, the set B is complete if and only if*
(A) $< \boldsymbol{k}; B >$ is simple and has no proper subuniverse and no proper automorphism,
(B) If $k = p^m$ for a prime p and $m \geq 1$ and if $< \boldsymbol{k}; + >$ is an elementary abelian p-group then some $b \in B$ does not preserve the quaternary relation

$$\{(x, y, z, x - y + z) \mid x, y, z \in \boldsymbol{k}\},$$

and
(C) If $k = h^m$ with $h > 2$ and $m > 1$ and T is an h-regular system on $\boldsymbol{k}$ then some $b \in B$ does not preserve λ_T.

Example. Let $k = 2$ (Boolean case). There are 4 nonunary minimal operations, namely, $\vee$, $\wedge$, d and r, where $\vee$ and $\wedge$ are OR and AND, $d(x, y, z) \approx (x \wedge y) \vee (y \wedge z) \vee (z \wedge x)$ and $r(x, y, z) \approx x \oplus y \oplus z$. With the unary non-identity operation $\neg$ (NOT), two pairs $(\neg, \vee)$ and $(\neg, \wedge)$ are shown to be gigantic. These are the only gigantic pairs for $k = 2$.

Next, we state that a gigantic pair really exists for every k which is not a power of 2.

Theorem 3. 3 *For every k where $k \neq 2^t$ $(t > 1)$, there exists a gigantic pair.*

Proof If k is a prime, the claim can be verified for the following two operations: Define $f(x) :\approx x \oplus 1$ and $g(x, y)$ such that $g(x, y) = x$ if $x = y$ and $g(x, y) = k - 1$ if $x \neq y$ for all $x, y \in \boldsymbol{k}$. It is easy to see that g is minimal; in fact, g is a semilattice join whose order is $0 \leq k - 1, \ldots, k - 2 \leq k - 1$.

Suppose that k is a composite number. Let p denote the greatest prime divisor of k and let $\ell := k/p$ where $\ell > 1$.

The following unary operation f and binary operation g on $\boldsymbol{k}$ suffice for our purpose.

We define f by setting

$$f(ip + j) := \begin{cases} ip + j + 1 & i \in \boldsymbol{\ell},\ 0 \leq j < p - 1, \\ ip & i \in \boldsymbol{\ell},\ j = p - 1. \end{cases}$$

Thus, f is expressed in the cyclic notation as

$$f = (0\ 1\ \cdots\ p-1)\,(p\ p+1\ \cdots\ 2p-1)\cdots((\ell-1)p\ \ (\ell-1)p+1\ \cdots\ k-1).$$

An algebra $\mathbf{A} = < \boldsymbol{k}; \vee >$ is a semilattice if the binary operator $\vee$ is associative, commutative and idempotent (*i.e.*, it satisfies

$$x \vee (y \vee z) = (x \vee y) \vee z,\ \ x \vee y = y \vee x \ \text{ and } \ x \vee x = x$$

for all $x, y \in \boldsymbol{k}$). The binary relation $\leq$ on $\boldsymbol{k}$ corresponding to $\mathbf{A}$ is defined by setting $a \leq b$ whenever $a \vee b = b$. It is well-known that $\leq$ is a partial order in which $a \vee b$ is the join of a and b. Conversely, an order $\leq$ on $\boldsymbol{k}$ in which each pair has a join determines a semilattice.

Let g be the following semilattice operator $\vee$ on $\boldsymbol{k}$. For every x, y in $\boldsymbol{k}$ set

$$x \vee y = \begin{cases} x & x = y, \\ (i+1)p & x = ip + j,\ \ y = ip + j' \\ & (0 \leq i \leq \ell - 2,\ \ 1 \leq j,\ j' \leq p - 1,\ \ j \neq j'), \\ 0 & \text{otherwise}. \end{cases}$$

The Hasse diagram of the order corresponding to the semilattice $< \boldsymbol{k}; \vee >$ is in Fig. 1. Notice that it is a tree.

The pair $(f, \vee)$ is proved to satisfy the conditions (i)–(vii) in Theorem 3.1 and so it is gigantic. □

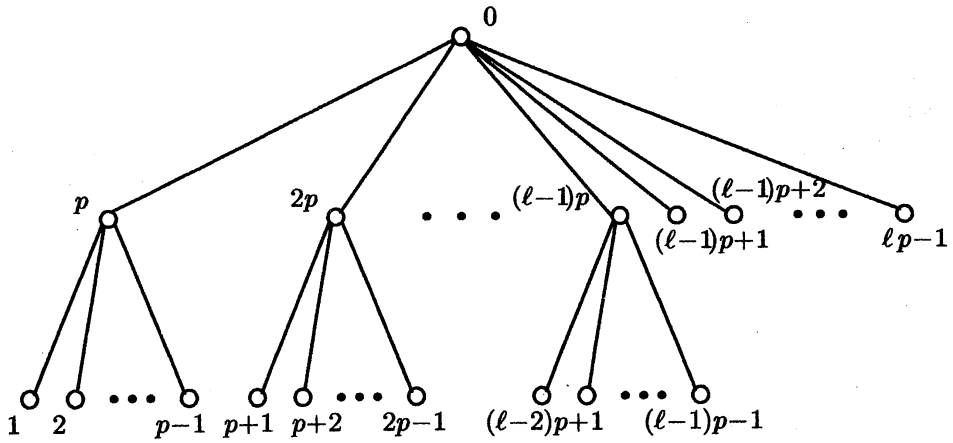

Figure 1: The semilattice for the operation $\vee$

References

[Cz 98] Czédli, G., Two minimal clones whose join is gigantic, Preprint, 1998.

[Cs 83] Csákány, B., All minimal clones on a three-element set, *Acta Cybernetica*, 6, 1983, 227-238.

[MR 93] Machida, H. and Rosenberg, I.G., Essentially minimal groupoids, in *Algebras and Orders*, Kluwer Academic Publishers, 1993, 287-316.

[PK 79] Pöschel, R. and Kalužnin, L.A., *Funktionen- und Relationenalgebren*, Deutscher Verlag der Wissenschaften, 1979.

[Qu 95] Quackenbush, R.W., A survey of minimal clones, *Aequat. Math.*, 50, 1995, 3-16.

[Ro 65] Rosenberg, I.G., La structure des fonctions de plusieurs variables sur un ensemble fini, *Comptes rendus de l'Acad. sci. Paris*, 260, 1965, 3817-3819.

[Ro 70A] Rosenberg, I.G., Über die funktionale Vollständigkeit in dem mehrwertigen Logiken, *Rozpravy Čs. Akademie Věd. Ser. Math. Nat. Sci. Praha*, 80, 4, 1970, 3-93.

[Ro 70B] Rosenberg, I.G., Complete sets for finite algebras, *Math. Nachr.*, 44, 1970, 253-258.

[Ro 86] Rosenberg, I.G., Minimal clones I: The five types, *Colloq. Math. Soc. J. Bolyai*, 43, 1986, 405-427.

[Sza 92] Szabó, L., On minimal and maximal clones, *Acta Cybernetica*, 10, 1992, 323-327.

[Sza 97] Szabó, L., On minimal and maximal clones II, *Acta Cybernetica*, Submitted.

[Sze 86] Szendrei, Á., *Clones in Universal Algebra*, Université de Montréal, 1986.